UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA	:	
- v. -	:	S3 17 Cr. 548 (JMF)
JOSHUA ADAM SCHULTE,	:	
Defendant.	:	

GOVERNMENT'S OPPOSITION TO DEFENDANT'S *PRO SE* BAIL MOTION

DAMIAN WILLIAMS
United States Attorney
Southern District of New York

David W. Denton, Jr.
Michael D. Lockard
Assistant United States Attorneys
- *Of Counsel* -

TABLE OF CONTENTS

Page

PRELIMINARY STATEMENT 1

BACKGROUND 1

A. The Defendant's Theft and Transmission of National Defense Information 1

B. The Defendant's Receipt and Possession of Child Pornography 8

C. The Charges and Bail Proceedings 9

D. Imposition of SAMs Based On the Defendant's Continued Transmission of National Defense Information and Violation of Protective Orders 12

E. The First Trial 14

DISCUSSION 15

I. Applicable Law 15

II. Discussion 16

A. The Defendant's Request to Reopen His Bail Hearing Should Be Denied 16

B. The Length of Pretrial Detention is not Unconstitutionally Excessive 18

C. Conditions of Pretrial Confinement 24

CONCLUSION 25

TABLE OF AUTHORITIES

Page

Federal Cases

Bell v. Wolfish, 441 U.S. 520 (1979) 15, 16
United States v. Briggs, 697 F.3d 98 (2d Cir. 2012).....19
United States v. El-Gabrowny, 35 F.3d 63 (2d Cir. 1994).....19
United States v. El-Hage, 213 F.3d 74 (2d Cir. 2000).....16, 19, 23
United States v. Hare, 873 F.2d 796 (5th Cir. 1989).....15
United States v. Hill, 462 F. App'x 125 (2d Cir. 2012).....21
United States v. Norton, 455 F. App'x 932 (11th Cir. 2012).....22
United States v. Petrov, 2015 WL 11022886 (S.D.N.Y. Mar. 26, 2015) 15
United States v. Schulte, No. 18-145 (2d Cir. Mar. 6, 2018).....12
United States v. Schwanborn, 249 F. App'x 906 (2d Cir. 2007) 18
United States v. Valerio, 9 F. Supp. 3d 283 (E.D.N.Y. 2014) 23
United States v. Whitworth, 856 F.2d 1268 (9th Cir. 1988) 22
Wilson v. C.I.A., 586 F.3d 171 (2d Cir. 2009) 20

Statutes

18 U.S.C. § 403.....14
18 U.S.C. § 793.....22
18 U.S.C. § 1001.....14
18 U.S.C. § 1030.....22
18 U.S.C. § 3142.....1, 15, 16, 22
18 U.S.C. § 3500.....16

PRELIMINARY STATEMENT

The Government respectfully submits this memorandum in opposition to the defendant's *pro se* motion for bail (the "Motion").[1] In the Motion, the defendant argues that that bail is warranted under the 18 U.S.C. § 3142 factors and that his pretrial detention violates the Due Process Clause of the Fifth Amendment and. For the reasons discussed below, the motion should be denied.

BACKGROUND

The charges in this case stem from the defendant's theft of classified documents and records (the "Classified Information") from the Central Intelligence Agency ("CIA") and his transmission of that classified information to WikiLeaks for publication. Between March 7 and November 17, 2017, WikiLeaks made 26 separate disclosures of classified CIA information (together, the "Leaks"). The Leaks contained, among other things, highly sensitive CIA information, including detailed descriptions of certain cyber tools used by CIA operators. The Leaks' impact on the CIA's intelligence gathering activities and the national security of the United States was catastrophic. The investigation of Schulte's theft and transmission of classified information revealed that he also received and possessed huge volumes of child pornography.

A. The Defendant's Theft and Transmission of National Defense Information

Schulte is a former employee of the CIA, where he worked in a group that developed cyber tools for other CIA components, the Operations Support Branch ("OSB") of the Engineering and

[1] The Motion is dated August 24, 2021, and was filed with the Classified Information Security Officer on September 30, 2021. The Motion also includes a request for a petition for a writ of habeas corpus pursuant to 28 U.S.C. § 2241 (Mot. 6-7 & 8-48). By order dated October 6, 2021, the Honorable Paul A. Crotty, United States District Judge, denied the Motion with respect to the petition for a writ of habeas corpus and directed the Government to respond to the Motion with respect to bail by October 21, 2021. (D.E. 526).

Development Group ("EDG"). OSB conducted its cyber development work on an internal CIA network called DEVLAN, which contained highly sensitive and classified national defense information concerning, among other things, the CIA's cyber tool arsenal. (Tr. 227; Tr. 597-601; GX 1062).[2] The CIA protected DEVLAN by restricting outside access to it; sequestering it from the Internet; limiting access to approximately 200 individuals, each of whom possessed a Top Secret security clearance; requiring badges to enter the locked rooms secured by vault doors in which DEVLAN terminals were stored; and protecting the CIA building in which the system was housed with armed guards and perimeter fencing. (*See* Tr. 187, 194-96, 213, 552, 779, 900-01, 907).

1. CIA's Reassignment of Schulte to a Different Branch and His Attempts to Restore Lost Administrator Privileges

In early 2016, following an internal personnel dispute, CIA reassigned Schulte and another employee to different branches within EDG to separate them. As part of his reassignment, Schulte's administrative privileges to two of his former branch's projects were revoked. (GX 1202-1; 1207-53; Tr. 976-80). Schulte complained that he was being unfairly retaliated against for making a personnel complaint. (GX 1039, 1046, & 506).

On April 14, Schulte secretly used his administrative privileges to another suite of development tools, called Atlassian, to restore his privileges to one of the projects, named OSB Libraries. (GX 1207-97). Schulte's actions were in direct violation of CIA policy and called into question whether Schulte could be trusted with classified information. (Tr. 297-99; 577-601; GX 1062). CIA issued a warning to Schulte (Tr. 609-14; GX 1095), who nonetheless attempted (again)

[2] In this memorandum, "D.E." refers to entries in the electronic docket, "Tr." refers to the trial transcript, "GX" refers to Government Exhibits introduced at trial, and "[Date] Tr." refers to the transcript of proceedings held on the specified date.

to get back his administrative privileges to OSB Libraries by falsely telling a colleague that his supervisors had authorized it. (Tr. 1508-09, 1620-21).

2. CIA's Reorganization of Administrator Privileges to Close the Backdoor Exploited by Schulte

CIA also decided to remove OSB developers from administrator roles in the DEVLAN servers and programs so that the security risk exploited by Schulte could not recur. Another developer, Jeremy Weber, and two other system administrators, David and Tim, were directed to remove all developers' administrative privileges to the Atlassian services on DEVLAN, including Schulte's. (Tr. 300-02; 792-804). David and Tim made the changes on a Saturday, April 16, 2016. (Tr. 792-804). David and Tim first created a "snapshot" of a DEVLAN database called "Confluence" (the "April 16 Snapshot"). (*Id.*; *see also* GX 1207-92; GX 1703 at 51-66). The April 16 Snapshot was a copy of the Confluence database as it existed on April 16 so that if any of the changes to the system caused problems going forward, David and Tim could restore the system and start over without doing lasting damage. (*Id.*). Because of the April 16 changes, Schulte could no longer access the Atlassian programs directly as a system administrator and, thus, no longer had access to, among other things, other system backups (the "Backup Files"). (*Id.*).

While the April 16 changes removed Schulte's (and other developers') administrator privileges to various programs and services, the administrative password and login credentials called "SSH keys" to the OSB physical server that hosted the Confluence Atlassian service were not changed. (Tr. 804; 937). An employee with the SSH keys could log in to the OSB server as an administrator using the administrative password, which would allow them to create, delete, or revert virtual servers such as Confluence; as well as to view, edit, and delete administrative log files, such as files showing who accessed the server and when. (Tr. 945-46, 966, 989-96). Although Schulte was, by early April, no longer a member of OSB and had no administrative role on the

OSB server, he nevertheless secretly continued to login using the administrative password and his SSH key (the "Schulte Key"). (Tr. 989-96). As described below, Schulte would use his OSB server access to restore his administrative privileges to the Atlassian services, navigate to the Backup Files to steal the Leaked Information, and delete and attempt to delete evidence of his activities.

After receiving the warning for abusing his administrator privileges to the OSB Libraries, and again after being notified about changes to administrator privileges to other DEVLAN services, Schulte tried to access DEVLAN as a system administrator, knowing that he was prohibited from doing so. Schulte successfully logged into the OSB server as an administrator multiple times, and thus knew that he still also had access through the Schulte Key. (Tr. 1014-23; GX 1203-16, 1207-26, 1209-17, 1209-20, 1209-9, 1209-3, 1209-18, 1209-19). On April 14, 2016, Schulte emailed a supervisor, Anthony Leonis, falsely reporting that he had "verified that all private keys with access have been destroyed/revoked" and that "[i]t seemed like overnight all my permissions within the products were removed and all my permissions on the servers themselves revoked. And all without anyone informing me." (GX 1063). At the same time, however, Schulte was logged into the OSB server as an administrator.

On April 18, Leonis emailed staff (including Schulte) to inform the group that going forward there would only be two system administrators for the Atlassian services, who were assigned to a different branch within EDG. (GX 1065). That evening, Schulte used his remaining administrative privileges on the OSB server to view log files generated by the OSB server that documented (i) information about every computer command (*i.e.*, instructions to the computer) that was entered into the system, such as the date and time of the command, and (ii) all login attempts to the server. (Tr. 1038-48; GX 1209-13, 1203-43, 1209-44, 1209-8). By reviewing these files, Schulte was able to see precisely what activity the system would record. (*Id.*). After Schulte

viewed the log files, he locked the vault on his floor, meaning that he was the last one in the vault around the time that he was using unauthorized access to view the log files. (GX 105).

On April 20, 2016, the EDG staff, including Schulte, was informed by email that on April 25, 2016, Confluence and another Atlassian service called "Bamboo" would be moved from the fOSB server to a new server. (GX 1067 and 1069). This was a significant change, as a result of which Schulte, would no longer be able to use the Schulte Key to access Confluence through the OSB server, and would no longer be able to use his OSB server access to restore his revoked administrator privileges to DEVLAN services.

3. Schulte's Theft of CIA National Defense Information Before the Backdoor was Closed

On April 20 at 5:30 p.m., Schulte used his administrative account on the OSB server to create a snapshot of Confluence titled "bkup." (GX 1202-17, 1209-7). A few minutes later, at 5:35 p.m., Schulte used that same account to revert Confluence to the April 16 Snapshot—*i.e.*, to a state before the removal of Schulte's administrative privileges. (GX 1202-18; Tr. 1063-65, 1073-75). While Confluence was in this reverted state, Schulte used his restored administrator privileges to copy two specific Confluence backup files created on March 3, 2016 (the "March 3 Backup Files"). (*Id*. at 953-58; GX 1207-27, 1207-30). The March 3 Backup Files contained the exact files that WikiLeaks later posted online beginning March 7, 2017. (Tr. 1113-33; Tr. 1351-66).

After a little more than an hour, Schulte then re-reverted Confluence back to the "bkup" state, *i.e.*, its April 20, 2016 state; deleted the records of his conduct; and then deleted the "bkup" snapshot that he had created earlier that day. (GX 1202-19, 1202-21; Tr. 1064-66). To further cover his tracks, Schulte systematically deleted log files on the OSB server that recorded his activities. (Tr. 1068-99; GX 1203-1, 1203-2, 1203-66, 1203-29, 1203-64, 1203-65, 1203-61). Schulte deleted the OSB server log files using the administrative session he had opened using the

Schulte Key, which was password protected with "KingJosh3000," a password used by Schulte, and tied to the unique IP address associated with Schulte's DEVLAN computer. (Tr. 1040-1050).

Over the next two weeks, Schulte continued to attempt to cover up his crime and eventually transmitted the Leaked Information to WikiLeaks from his home. On the morning of April 21, 2016, Schulte emailed Leonis to remove Schulte's access to the OSB server—the same server he had broken into the night before to steal the Classified Information. (GX 1071). Less than an hour later, Schulte erased the logs and contents of a USB device that had been plugged into his DEVLAN workstation on April 20, 2016, when he stole the Classified Information. (GX 1205-1).

4. Schulte's Transmission of CIA National Defense Information to WikiLeaks

While Schulte was covering up his activities at the CIA, at home, he was preparing to send the Classified Information to WikiLeaks, including downloading programs to covertly transfer the data and to securely delete evidence of his conduct. (GX 1404-6; Tr. 1372-75, 1389-93). On April 24, Schulte ordered for same-day delivery equipment to transfer data from external hard drives (GX 1305-6; Tr. 1377-78), like the hard drives that were recovered from Schulte's apartment by the Federal Bureau of Investigation ("FBI") following the Leaks. (GX 1603, 1609, and 1610; Tr. 1378-79). That same day, Schulte also downloaded Tails, a program that facilitates the anonymous transfer of information over the Internet and is recommended by WikiLeaks to be used, in conjunction with the program TOR—which was also installed on Schulte's home computer—to securely transmit sensitive information. (GX 1403-7 and 1702; Tr. 1382-83).

Schulte transferred the Classified Information overnight on April 30 into May 1, 2016. On April 30 at 11:28 a.m., Schulte downloaded a program that securely deletes data so that it is impossible to recover. (GX 1402-10; Tr. 1393-96). Later that night, Schulte searched on several occasions for secure wiping utilities and visited related websites, including a website titled "Kill

Your Data Dead With These Tips and Tools." (GX 1305-9; Tr. 1408-09). At 12:19 a.m. on May 1, Schulte mounted a drive containing certain encrypted files onto his home computer's virtual machine to transfer the Classified Information. (GX 1401-1). Over the next several hours through the middle of the night and early morning, Schulte repeatedly unlocked his computer to check on the status of that transfer. (GX 1401-1). Then, at approximately 3:18 a.m. on May 1, Schulte searched several times for information about "hashing" large files (a technique to confirm the integrity of transferred data) and visited related websites, such as "What is the fastest way to hash md5 large files" and "how can I verify that a 1tb file transferred correctly." (*Id.*).

On May 5, 2016, after having transferred the Classified Information, Schulte reformatted his home computer, including the drive that contained the encrypted files. This had the effect of erasing these drives. (Tr. 1409).

Due to the format of the Classified Information, it would have taken WikiLeaks a substantial amount of time to prepare it for public dissemination. (Tr. 1113-33). A few months after Schulte transmitted the Leaked Information, Schulte began regularly searching for information about WikiLeaks. In the six years prior to August 2016, Schulte had conducted three Google searches for WikiLeaks material and visited nine related webpages. (GX 1351). Between August 2016 (approximately three or four months after he stole the Leaked Information) and January 2017, Schulte conducted at least 39 Google searches for WikiLeaks and related terms and visited 115 related webpages. (GX 1352). Schulte even searched "WikiLeaks Code." WikiLeaks had never before published source code, but the Backup Files that Schulte had stolen contained source code, some of which was eventually disclosed in the Leaks. (GX 1, 1352; Tr. 174-75; 2272). In addition, on January 4, 2017, Schulte searched for "WikiLeaks 2017" and visited a webpage titled "WikiLeaks Vows to 'Blow You Away' in 2017 'Showdown.'" (GX 1352).

5. WikiLeaks' Publication of National Defense Information Stolen By Schulte

On March 7, 2017, WikiLeaks posted the first of the Leaks online. The first Leak contained Confluence information from the March 3 Backup Files, the same files Schulte copied on April 20, 2016. (GX 1; Tr. 174; 1113-33; 1350-66). In subsequent releases, the last of which occurred on or about November 17, 2017, WikiLeaks posted data about CIA cyber tools, including source code. (GX 1; Tr. 174-76). From the day of the initial Leak until March 14, 2017, Schulte conducted 28 searches related to the Leak and visited 91 webpages, including a search for "WikiLeaks public opinion." (GX 1353). Schulte also searched on at least six occasions for the "FBI" and visited webpages titled "FBI Prepares Hunt for the Source of CIA Documents," "WikiLeaks Reveal CIA Hacking Trove, Has Feds on Mole Hunt," and "FBI Joins CIA in Hunt for Leaker." (*Id.*).

6. Schulte's Lies to the FBI

In the FBI's investigation of the Leaks, Schulte was interviewed on several occasions, and repeatedly lied about his conduct. For example, Schulte falsely (i) denied being responsible for the Leaks; (ii) denied having a copy of a classified email (a copy of which was recovered by the FBI from Schulte's apartment (GX 1616)); (iii) denied taking information from DEVLAN to his home (even though he explicitly said in chats with friends that he took information from DEVLAN to his home and knew it was wrong (GX 1405-5; Tr. 2238-39, 2242-46)); and (iv) denied ever making DEVLAN vulnerable to theft (even though he systematically deleted DEVLAN log files on April 20, 2016 and otherwise repeatedly misused his administrator privileges on the system (GX 1062; Tr. 291-301; 576-601)). Moreover, despite being asked repeatedly about his DEVLAN activities, Schulte never mentioned anything related to his activities on April 20, 2016. (Tr. 2178).

B. The Defendant's Receipt and Possession of Child Pornography

In March 2017, the FBI searched Schulte's residence in New York pursuant to a search warrant and recovered, among other things, multiple computers, servers, and other electronic

storage devices, including Schulte's personal desktop computer (the "Desktop Computer"). (Complaint ¶ 2). On the Desktop Computer, FBI agents found an encrypted container (the "Encrypted Container") containing over ten thousand images and videos of child pornography (the "CP Files"). (*Id*. ¶ 3(a), (c)). For example, one file was a video depicting a prepubescent female approximately three-to-six years old engaging in various sex acts. (*Id*. ¶ 3(e)(ii)). The Encrypted Container containing the CP Files was identified by FBI computer scientists beneath three layers of encryption. (Complaint ¶ 4). Each layer of encryption was unlocked using passwords previously used by Schulte on one of his cellphones. (*Id*.). FBI agents also identified Internet chat logs in which Schulte and others discuss their receipt and distribution of child pornography. (*Id*. ¶ 5). Schulte also conducted a series of Google searches for child pornography. (*Id*. ¶ 6).

Finally, during an interview with law enforcement on June 26, 2017, Schulte admitted that the Desktop Computer was his primary computer; Schulte was the sole and exclusive user of the Desktop Computer; he had personally installed encryption software on the Desktop Computer; and he did not share the password for the encrypted portions with anyone else. (*Id*. ¶ 7).

C. The Charges and Bail Proceedings

Schulte was charged by complaint and arrested on August 24, 2017, based on three counts related to his possession, receipt, and interstate transportation of over ten thousand images of child pornography. (D.E. 1). During Schulte's presentment on the Complaint, the Government argued for detention on the grounds that the defendant is both a danger to the community and a flight risk. As relevant here, the Government discussed several photographs recovered from the defendant's cellphone that depicted an unknown individual using his hands to sexually assault an unconscious woman (the "Victim"). (*See* Aug. 24, 2017 Tr. at 12-13). At the time, the Government was aware

that the Victim knew the defendant and had lived in his apartment as a roommate in the past. (*Id.*).[3] Magistrate Judge Henry B. Pitman, who presided over the presentment, did not consider the information proffered by the Government regarding the Victim, explaining that "facts have [not] been proffered that . . . tie Mr. Schulte to the conduct in that incident." (*Id*. at 48-89). Nevertheless, Judge Pitman detained the defendant concluding that the defendant had not rebutted the presumption that he was a danger to the community. (*Id*. at 47-49).

On September 6, 2017, a grand jury returned an indictment containing the same charges included in the complaint, and the defendant was arraigned on September 13, 2017. During the arraignment, the defendant moved again for bail, arguing that any risk of danger would be "completely negated" if the defendant were denied access to a computer while on supervised release. (*See* Sept. 13, 2017 Tr. at 17, 26, 28-29). In response, the Government explained that the defendant is highly sophisticated with computers and that there were no set of conditions that could ensure that he would not attempt to circumvent bail restrictions and access the Internet. (*Id.* at 20, 22-25). After considering the parties' arguments and the position of Pretrial Services, the Court released the defendant, imposing strict conditions including, among others, home incarceration and no use of computers or the Internet in the absence of express authorization from Pretrial Services. (D.E. 8). The defendant met his bail conditions and was released on September 15.

On or about November 15, 2017, the defendant was charged in Loudoun County Virginia with two crimes: (i) object sexual penetration, a felony, in violation Virginia Code Section 18.2-67.2; and (ii) the unlawful creation of an image of another, a misdemeanor, in violation of Virginia Code Section 18.2-386.1. The Government understands that these charges are premised on the

[3] The defendant has called the Victim his "girlfriend." (*E.g.*, Mot. 2, 60). Even if that were true, it is not a defense to sexually assaulting an unconscious person. But, contrary to the defendant's claims, the Government believes the Victim was never the defendant's girlfriend.

photographs of the Victim. Specifically, the Loudoun County Commonwealth Attorney's Office has developed evidence that the defendant was the individual whose hands are visible in the photographs sexually penetrating the Victim.

The Government also obtained evidence that Schulte continued to use the Internet in violation of his conditions of release. First, data from the service provider for the defendant's email account showed that the account was regularly logged into and out of while the defendant was released on bail. The IP address used to access Schulte's email was almost always the same IP address associated with the broadband internet account for the defendant's apartment (the "Broadband Account"). Moreover, data from the Broadband Account showed that on November 16, 2017, the Broadband Account was used to access the "TOR" network, that is, a network that allows for anonymous communications on the Internet via a worldwide network of linked computer servers, and multiple layers of data encryption. The Broadband Account showed that additional TOR connections were made on November 17, 26, 30, and December 5, 2017.

On December 7, 2017, the Government moved to revoke the defendant's bail. D.E. 21. On December 14, 2017, Schulte consented to detention without prejudice to later challenging the Government's motion for detention. (Dec. 14, 2017 Minute Entry). On January 8, 2018, Schulte argued again for bail. At the bail hearing, Schulte's counsel argued that Schulte used the TOR network because "Mr. Schulte is writing articles, conducting research and writing articles about the criminal justice system and what he has been through, and he does not want the government looking over his shoulder and seeing what exactly he is searching." (Jan. 8, 2018 Tr. at 15). After considering the parties' arguments, Judge Crotty denied Schulte's application, finding that Schulte had violated his bail conditions by directing his roommate to use the Internet on Schulte's behalf and that Schulte was a danger to the community. (*Id.* at 16). Schulte appealed the detention order

to the Court of Appeals for the Second Circuit, and the Court affirmed. *See United States v. Schulte*, No. 18-145 (2d Cir. Mar. 6, 2018).

D. Imposition of SAMs Based On the Defendant's Continued Transmission of National Defense Information and Violation of Protective Orders

On June 18, 2018, the defendant was charged in a thirteen-count Indictment with espionage and other offenses related to the Leaks, as well as child pornography and copyright offenses. *See* D.E. 47.

After Schulte was detained at the MCC, he and other inmates arranged to have cellphones (the "Contraband Cellphones") illegally smuggled into the prison for their use. Schulte coordinated his activities with other inmates, often using other inmates to obtain or store the Contraband Cellphones and using the Contraband Cellphones to pass messages covertly to other inmates. (*See* D.E. 96, Ex. A). Schulte used the Contraband Cellphones to access encrypted email accounts (the "Encrypted Email Accounts") and social media accounts (the "Social Media Accounts"). In his own words, Schulte intended to use these accounts to engage in an "information war" with the United States by systematically disclosing classified information and materials designed to obstruct the investigation and prosecution. For example, in journals found in Schulte's MCC cell, Schulte wrote the following:

- "If govt doesn't pay me $50 billion in restitution & prosecute the criminals who lied to the judge and presented this BS case then I will visit every country in the world and bear witness to the treachery . . . that is the USG [United States Government]. I will look to breakup diplomatic relationships, close embassies, and U.S. occupation around the world & finally reverse U.S. jingoism. If this is the way the U.S. govt treats one of their own, how do you think they treat allies?"

- "I NEED my discovery to be released to the public. I NEED my articles to be updated."

- "The way is clear. I will set up [two blogs]. From here, I will stage my information war: . . . The [blog] will contain my 10 articles . . . ."

Schulte's "information war" was no idle musing. Schulte used the Encrypted Email and Social Media Accounts to disseminate and attempt to disseminate classified information. For example, using one of the Encrypted Email Accounts, Schulte corresponded with a reporter. Pretending to be a third person speaking on Schulte's behalf, Schulte told the reporter that he would give the reporter "information" on several topics—including disclosures relating to high-ranking elected officials in the United States—if the reporter published stories in accordance with a timeframe dictated by Schulte. In another September 2018 email, Schulte attached a copy of one of the search warrants, even though Schulte previously had confirmed his understanding that a protective order prohibited this type of dissemination. Schulte also attached a document in which he disputed facts contained in the search warrant, in which he included classified information.

Using the Contraband Cellphones, Schulte also began to post his writings on some of the Social Media Accounts. In these posts, Schulte claimed, among other things, that the Government had planted child pornography on his computer and that, through this prosecution, the "United States government has done the job of a foreign adversary to exploit its own intelligence officers." Although the Government seized the Contraband Cellphones before Schulte was able to complete his plan, Schulte's journals make clear that he intended to disseminate other classified information. For example, Schulte's journals include (1) a draft WikiLeaks article authored by a supposed FBI "whistleblower," claiming that the FBI leaked Schulte's discovery to WikiLeaks and that Schulte had been framed by the FBI; (2) drafts of tweets purportedly written by one of Schulte's former CIA colleagues, which disclosed classified information to bolster the alleged former colleague's credibility and which claimed knowledge that Schulte had been framed by the CIA; and (3) a draft "article" in which Schulte criticized the FBI's investigation and included classified information about Schulte's training at the CIA. Based on the defendant's conduct, on October 31, 2018, the

Government filed a second superseding indictment charging him with two additional counts of unlawfully disclosing and attempting to disclose classified information and contempt of court for willfully violating a court order. (*See* D.E. 68).

The Attorney General also authorized the imposition of Special Administrative Measures ("SAMs") to prevent Schulte from further unlawful disclosures of national security information. (*See* D.E. 127 at 1, 3-4). On May 10, 2019, Schulte moved to vacate the SAMs, arguing that they violated his due process rights and were not reasonably necessary to prevent the disclosure of classified information. (*See* D.E. 92; D.E. 127 at 1). Judge Crotty upheld the SAMs, with two minor modifications, finding that: "The SAMs are undoubtedly restrictive, but generally they are reasonably necessary to avoid further disclosure of classified information. Despite escalating restrictions on Schulte's freedom prior to his isolation in 10 South, Schulte continued to flout Court orders and his bail conditions, protective order, BOP rules, and procedures for handling classified information." (*Id*. at 8). On June 24, 2021, Schulte filed a second, *pro se*, motion to vacate the SAMs, which Judge Crotty again denied. (D.E. 527). Judge Crotty held that "these measures, although hard, are '"reasonably related" to legitimate penological objectives' so long as Schulte is facing trial for substantial espionage charges, handling and reviewing sensitive classified material in discovery as he prepares his *pro se* defense, and continuing his troubling pattern of disrespect for the Court's protective orders and other directives regarding classified information." (*Id*. at 3).

E. The First Trial

On February 2, 2020, trial began as to the eleven national-security-related counts in the S2 Indictment. On March 9, 2020, a jury found the defendant guilty of two of those counts: making false statements to law enforcement, in violation of 18 U.S.C. § 1001, and contempt of Court, in violation of 18 U.S.C. § 401(3). These counts related to Schulte's lies to FBI during its investigation of the Leaks and his violation of the Protective Order by disclosing protected

materials to third parties. The jury was unable to reach a unanimous verdict as to the remaining eight counts, and the Court granted the defendant's motion for a mistrial as to those counts.

On June 8, 2020, the Government sought and obtained a third superseding indictment from a Southern District grand jury sitting in White Plains. (*See* D.E. 405). The S3 Indictment contains nine counts that are based on the same conduct that was at issue during the February 2020 trial, namely, the defendant's theft and transmission of the Classified Information, his destruction of log files and other forensic data on CIA computer systems in the course of committing that theft, his obstruction of the investigation into the Leaks, and his transmission and attempted transmission of national defense information while detained in prison.

DISCUSSION

I. Applicable Law

Under 18 U.S.C. § 3142(f), the court may reopen a detention hearing "at any time before trial if the judicial officer finds that information exists that was not known to the movant at the time of the hearing and that has a material bearing on the issue whether there are conditions of release that will reasonably assure the appearance of such person as required and the safety of any other person and the community." "A court may properly reject an attempt to reopen a detention hearing where the new information presented is immaterial to the issue of flight risk or danger to the community." *United States v. Petrov*, No. 15 Cr. 66 (LTS), 2015 WL 11022886, at *2 (S.D.N.Y. Mar. 26, 2015) (citing *United States v. Hare*, 873 F.2d 796, 799 (5th Cir. 1989)).

"In evaluating the constitutionality of conditions or restrictions of pretrial detention that implicate only the protection against deprivation of liberty without due process of law, we think that the proper inquiry is whether those conditions amount to punishment of the detainee." *Bell v. Wolfish*, 441 U.S. 520, 536 (1979). Where a defendant has been lawfully detained prior to trial following a bail hearing, "the Government concededly may detain him to ensure his presence at

trial and may subject him to the restrictions and conditions of the detention facility so long as those conditions and restrictions do not amount to punishment, or otherwise violate the Constitution." *Id.* Restrictive conditions of confinement do not violate due process where they are "'reasonably related' to legitimate penological objectives," as opposed to "an 'exaggerated response' to those concerns." *United States v. El-Hage*, 213 F.3d 74, 81 (2d Cir. 2000).

"To determine whether the length of pretrial detention has become unconstitutionally excessive, a court must weigh: (1) its length, (2) the extent of the prosecution's responsibility for delay of the trial, (3) the gravity of the charges, and (4) the strength of the evidence upon which detention was based, *i.e.*, the evidence of risk of flight and dangerousness." *Id*. at 79 (cleaned up).

II. Discussion

A. The Defendant's Request to Reopen His Bail Hearing Should Be Denied

The defendant argues that his detention hearing should be reopened under § 3142(f) because he has discovered "new information" that, he contends, shows that his state prosecution for sexual assault was improperly engineered by the FBI for purposes of causing his bail to be revoked. (Mot. 58-61).[4] The defendant relies on certain emails produced pursuant to 18 U.S.C. § 3500. (Mot. Ex. C). The defendant's argument should be rejected because (1) the proffered information is not "new" and, indeed, was discussed at the defendant's January 8, 2018 bail hearing; (2) the record shows only legitimate law enforcement actions; and (3) even if the defendant's proposed interpretation were correct, it would not be "material" in view of the overwhelming evidence of the danger the defendant poses to the community.

[4] This memorandum does not address the defendant's bail arguments made in the context of his request for a writ of habeas corpus (Mot. 8-48), which was denied by the court's order dated October 6, 2021. (D.E. 526).

As described above, in the course of the investigation of Schulte's theft and transmission of classified information, the FBI also obtained evidence of Schulte's receipt and possession of massive quantities of child pornography and his commission of a sexual assault on the unconscious Victim. (*Supra* 8-11). That evidence was provided, as it should have been, to law enforcement authorities with jurisdiction to investigate and prosecute the crime and to protect the interests of a victim of sexual assault. The Loudoun County, Virginia, Office of the Commonwealth Attorney (the relevant prosecutorial office) determined that the evidence was sufficient to show that the Victim was sexually assaulted and that Schulte committed the sexual assault. (Mot. Ex. C).

Schulte's argument is not based on new information. The Government discussed the photographs of the defendant's sexual assault at his August 24, 2017 presentment. (*Supra* at 9-10). The circumstances under which the state charges were brought, and defense counsel's contention that they were engineered by the FBI for bail purposes, were discussed at his January 8, 2018 bail hearing, and defense counsel contended that "the Virginia case is just a means to keep Mr. Schulte detained . . . [T]he FBI just gave [the photographs] to Virginia and asked them to make an arrest." (Jan. 8, 2018 Tr. at 5-6). Defense counsel also argued that the Victim "still cannot identify Mr. Schulte." *Id*.[5] The Motion merely rehashes precisely these same arguments, and does not raise any "information . . . that was not known to the movant at the time of the hearing."

The emails cited in the Motion do not materially add to this record, and certainly do not support the defendant's long-standing claim that the state charges were engineered. The defendant principally focuses on a statement by a Detective in the Loudoun County Sherriff's Office about

[5] In his Motion, Schulte argues that the Victim "specifically state[s] Mr. Schulte was not involved in any sexual assault," which is a clear mischaracterization of the facts. The Victim's inability to identify the person who assaulted her while she was unconscious in no way exonerates the defendant.

whether or not the pictures show penetration. (Mot. 59). The defendant could have argued the probity of those photographs at his prior bail hearing. Moreover, the Detective's opinion about the pictures is not determinative, and the relevant prosecution office disagreed. The Commonwealth Attorney concluded that the evidence showed felony sexual battery and felony digital penetration, and that Schulte was the offender. (Mot. Ex. C).

Finally, Schulte's proffered "new information" is not material in light of the overwhelming evidence of the danger he poses to the community. *See, e.g.*, *United States v. Schwanborn*, 249 F. App'x 906, 907 (2d Cir. 2007) (summary order) ("the new evidence offered by Schwanborn is not reasonably likely to affect the outcome of the proceeding as multiple instances of threats remain unrebutted"). As discussed above, the evidence of Schulte's dangerousness includes not only his commission of sexual assault, but also his receipt and possession of enormous quantities of child pornography, his sophisticated theft and dissemination of masses of classified information, his lying to the FBI, his violations of protective orders, and his continued disclosures and attempted disclosures of classified information, even from prison. The danger he poses requires detention, as well as the imposition of restrictive SAMs that have been twice upheld by the court. This conduct is reflected in the charges against him, the Attorney General's findings in authorizing the imposition of the SAMs, and the jury's verdicts of guilty on charges of lying to the FBI and violating the court's orders.

Accordingly, the defendant's request to reopen his detention hearing should be denied.

B. The Length of Pretrial Detention is not Unconstitutionally Excessive

Schulte's argument that the length of his pretrial detention is unconstitutionally excessive should also be denied.

Length. "While the length of pretrial detention is a factor in determining whether due process has been violated, the length of detention alone is not dispositive and will rarely by itself

offend due process." *El-Hage*, 213 F.3d at 79 (internal quotation marks omitted). Here, Schulte has been detained since December 2017, a period of approximately 3 years and 10 months. During that time, a five-week trial was held from February 2 to March 9, 2020, at a time when the defendant had been detained for a period of approximately 25 months. That trial resulted in a guilty verdict on two of the counts. Following post-trial briefing and the defendant's motion to dismiss the third superseding indictment returned in June 2020, which the Court denied on March 24, 2021 (*see* D.E. 459), a trial on the charges in that indictment was scheduled for October 2021 at the joint request of the parties. *See* D.E. 458. The defendant then asked to waive his right to counsel and proceed *pro se*, which was granted after two *Faretta* hearings. (D.E. 485). Judge Crotty then adjourned the trial date at the defendant's request. (D.E. 517). A new trial date has not yet been set, but Judge Crotty expressed an intention to hold the trial in early 2022. (D.E. 552 at 5-6).

Although Schulte has been detained for a long period, the Second Circuit has recognized that "the importance and complexity of [a] case and the extensive evidence" can "reasonably require a lengthy period for pretrial preparation." *United States v. El-Gabrowny*, 35 F.3d 63, 65 (2d Cir. 1994). Although the Government must of course pursue even "a case of considerable complexity and scope . . . with promptness and energy," *United States v. Briggs*, 697 F.3d 98, 103 (2d Cir. 2012), as amended (Oct. 9, 2012), the unusual complexity of the facts of this case, the technical nature of much of the discovery, the sophisticated and extensive motion practice (including pursuant to the Classified Information Procedures Act), and the need to conduct a retrial provide sufficient explanation for the length of delay inherent in this case.

Responsibility for Delay. Schulte's attempts to assert that the Government is wholly responsible for the delay in this case are unavailing and frequently premised on misstatements of fact. First, Schulte claims that the Government failed to produce promptly the discovery in his case

prior to the first trial. Although the Government, as is its obligation, continued to produce discoverable materials to the defendant as they were identified, the vast majority of discovery (both classified and unclassified) was produced by the end of 2018. Schulte's claim that delay was caused by the Government's purported failure to produce "the forensic crime scene" (Mot. at 50-51, 52), merely reiterates Schulte's disagreements with the Court's orders denying Schulte's demands for the wholesale production of servers from the CIA (*see* D.E. 124, 514), rather than any failure by the Government to produce discovery to which Schulte is entitled. The same is true of Schulte's claim that he is entitled to an unclassified production of WikiLeaks files and other classified discovery, which was produced to him in classified discovery and which, the Court recognized, cannot be produced in unclassified form. (D.E. 513 at 3 (noting that "'evidence of public disclosure does not deprive information of classified status'" (quoting *Wilson v. C.I.A.*, 586 F.3d 171, 174 (2d Cir. 2009)); *see also* D.E. 546 (clarifying status of electronic discovery made available to the defendant in the SCIF)). More broadly, with respect to Schulte's generalized claims regarding the Government's responsibility for his purported inability to prepare for trial, the Court has already recognized that "Schulte has been afforded a suite of accommodations, including, *inter alia*, regular SCIF hours for classified discovery; access to legal research and unclassified discovery; special provisions expediting legal mail and correspondence from the Government; equipment, hardware, and other resources necessary to prepare his defense from the MCC; and standby counsel's assistance in briefing, arguing, corresponding, and filing." D.E. 552.[6]

Schulte also asserts that the delay should be attributed to the Government because he was not produced to the Courthouse SCIF to review classified discovery. Throughout much of 2020,

[6] As the Government has previously noted, Schulte has access to the unclassified discovery in this case on a laptop in his cell provided by his former counsel. (*See* D.E. 499 at 40).

the COVID-19 pandemic precluded access to the Courthouse, including the SCIF. The Government nevertheless worked diligently with the Classified Information Security Officer to see if alternative options were possible, including creating a new SCIF in U.S. Marshals' space, all of which Schulte's prior counsel declined. (*See, e.g.*, Aug. 17, 2020 Tr. at 5-7; Nov. 4, 2020 Tr. at 3, 5 (defense counsel averring that the "current SCIF is simply not a viable option")). Once defense counsel was once again prepared to use the Courthouse SCIF (*see* June 15, 2021 Tr. at 7), the Government promptly undertook to facilitate the necessary logistical arrangements, including supplementing U.S. Marshals' personnel with FBI agents to provide the necessary security, to facilitate Schulte's production to the SCIF. (*See* D.E. 471; 482).

As Schulte acknowledges, he and his former counsel have repeatedly sought adjournments of the retrial in this matter. Contrary to his representations, these were not the result of unwarranted delay on the part of the Government, but because "Mr. Schulte ha[d] a long list of things and tasks that he expects . . . to accomplish before a retrial" (Aug. 17, 2021 Tr. at 9), including Schulte's announced intention as of August 2, 2021, to file "at least 10 more pretrial motions." (D.E. 490 at 15). "Although the length of [Schulte's] detention certainly requires convincing justification for its continuance, that justification is found in the inherent complexities of this . . . case, which presents defense counsel with voluminous discovery to absorb and the court with myriad motions to address." *United States v. Hill*, 462 F. App'x 125, 127 (2d Cir. 2012). The Government has consistently sought to proceed with scheduling a retrial as expeditiously as possible. (*See, e.g.*, Aug. 17, 2020 Tr. at 4-5; Nov. 4, 2020 Tr. at 2). "[T]he record reflects no intentional, unwarranted delay by the prosecution, and most of the delay is attributable to the continuances requested by [the defendant and his former counsel] and the complexities inherent in [this] case." *Hill*, 462 F.

App'x at 127. Accordingly, the Court should not find that the delay in this matter is attributable to the Government.

Gravity of the Charges. Although Schulte blithely asserts that the charges here are non-violent, and therefore not serious, he is plainly incorrect. "Espionage is one of this nation's most serious offenses." *United States v. Whitworth*, 856 F.2d 1268, 1289 (9th Cir. 1988). The former Deputy Director of the CIA's Directorate of Digital Innovation testified at trial that the theft of information with which Schulte is charged "was the equivalent of a digital Pearl Harbor," and that once revealed by WikiLeaks, critical CIA "operations were immediately at risk, . . .[i]t immediately undermined the relationships we had with other parts of the government as well as with vital foreign partners, who had often put themselves at risk to assist the agency. And it put our officers and our facilities, both domestically and overseas, at risk." (Tr. 1844). Not only are the charged violations of 18 U.S.C. § 793 themselves serious, but the charged computer offenses, in violation of 18 U.S.C. § 1030, must also be considered in context of those espionage crimes—as alleged in the Indictment, Schulte committed a range of computer crimes for the express purpose of enabling his crimes of espionage and then deleting evidence of his theft of extraordinarily sensitive classified information.

Although unrelated to the espionage offenses, the child pornography crimes with which Schulte is charged are also extremely serious crimes that carry substantial sentences if Schulte is convicted. *See, e.g.*, *United States v. Norton*, 455 F. App'x 932, 934 (11th Cir. 2012) ("Receiving child pornography is a serious crime that victimizes children."). For that reason, there is a presumption in favor of detention for those charged with child pornography crimes. *See* 18 U.S.C. § 3142(e)(3)(E). "The reason for this presumption is clear . . . child pornography is an insidious offense since it takes advantage of a particularly vulnerable segment of society, children." *United*

States v. Valerio, 9 F. Supp. 3d 283, 289 (E.D.N.Y. 2014) (internal quotation marks and citation omitted). Here, Schulte received, possessed, and transported thousands of images and videos of child pornography, some of which depicted sadistic or masochistic conduct involving children as young as a few years old, and Schulte used his technical skills to bury these images and videos beneath layers of encryption so that they were virtually undetectable by law enforcement.

Strength of the Proof. As described above, *see supra* at 1-10, the evidence of Schulte's guilt of the charged offenses is strong, and provides additional basis for his detention in advance of trial, even though that period has been lengthy. Moreover, the Second Circuit has instructed that in analyzing this factor, courts should consider not just the strength of the evidence of the defendant's guilt *vel non*, but specifically "the strength of the evidence upon which detention was based, *i.e.*, the evidence of risk of flight and dangerousness." *El-Hage*, 213 F.3d at 79. Judge Crotty repeatedly found, including within the last month, that Schulte continues to pose a danger to the community. "[T]here is an ongoing, present 'danger that [Schulte] will disclose classified information.'" (D.E. 552 at 3 (quoting D.E. 127 at 7)). Schulte "has been convicted of violating this Court's protective orders, and has intentionally disclosed information he knows to be classified—including in a recent publicly-filed motion seeking declassification of that very information," and has "continu[ed] his troubling pattern of disrespect for the Court's protective orders and other directives regarding classified information." (D.E. 527 at 2-3). If anything, the evidence that Schulte's dangerousness warrants his detention has only increased. "A longer pretrial detention is more justifiable for a defendant found to be dangerous than for a defendant who presents only a risk of flight." *El-Hage*, 213 F.3d at 80.

In sum, although the Government acknowledges the length of time for which Schulte has been detained, those delays are not the fault of the Government. They have resulted from the need

to conduct a complex retrial of extremely serious offenses during a global pandemic. As Judge Crotty recognized, Schulte continues to pose an unprecedented risk of the exposure of extremely sensitive classified information, and has literally shown his contempt for court orders designed to try and prevent that harm. No combination of conditions could ensure the safety of the community in the face of such recalcitrance. Accordingly, balancing all of the relevant factors, Schulte's continued detention pending trial in this matter does not offend due process.

C. Conditions of Pretrial Confinement

Schulte also reiterates his objections to the conditions of his confinement, asserting that they, too, provide a basis for his release. On the contrary, these arguments merely rehash Schulte's repeated challenges to the SAMs. The Court has also repeatedly rejected these claims. (*See* D.E. 527). Notwithstanding those restrictions, "the parties, the CISO, and the Court have spent countless hours conferring and, in many instances, resorting to motion practice to chart a just and workable course through the web of confidentiality complexities and SAMs constraints inherent to these proceedings." (D.E. 552 at 5). As the Court previously ordered, the Government will continue to make efforts to ensure that the accommodations to which Schulte has access are sufficient to ensure that he can adequately defend himself at trial.

CONCLUSION

For the foregoing reasons, the Government respectfully requests that the Court enter an order denying the Motion.

Dated: October 21, 2021
New York, New York

DAMIAN WILLIAMS
United States Attorney

By: /s/
David W. Denton, Jr. / Michael D. Lockard
Assistant United States Attorneys
(212) 637-2744 / -2193

To: Joshua Adam Schulte (by hand, via MDC Legal Department)
Standby Counsel of Record (by ECF)